

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |



NASA Procedural Requirements

COMPLIANCE IS MANDATORY

NPR 2810.1A

Effective Date: May
16, 2006
Expiration Date: May
16, 2011

[Printable Format \(PDF\)](#)

Request Notification of Change

(NASA Only)

Subject: Security of Information Technology

Responsible Office: Office of the Chief Information Officer

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) |
[Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) | [Chapter11](#) |
[Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) | [Chapter16](#) | [Chapter17](#) |
[Chapter18](#) | [Chapter19](#) | [Chapter20](#) | [Chapter21](#) | [AppendixA](#) | [AppendixB](#) |
[ALL](#) |

Chapter 8 Master and Subordinate IT Systems

8.1 Designation of Master and Subordinate IT Systems

8.1.1 NASA has organized its IT systems with its programmatic and institutional lines of business to comply with OMB and FISMA reporting requirements on IT systems and the OMB and NIST criteria for defining a system's accreditation boundary of responsibility to align with the terms used within NASA Structure Management (NSM). By following NASA's lines of business, IT systems align (1) the budget authority with the information security AO; (2) the mission and functional responsibilities with system ownership and managing risk; and (3) the performance objectives with operational characteristics and security needs. Since managing information security is mandatory for all IT systems and since IT systems have various SDLCs, NASA has established master-level systems to allow Agency- and program-level information security controls to be certified and accredited for all subordinate systems under each master system's authority. A Master system's decisions and security controls are inherited by its subordinate systems.

8.1.2 Master systems can be comprised of a single MA or a MEI system. Master plans may also establish information security requirements for many subordinate GSSs. Designated AOs establish high-level master systems. Following the certification process, the AO accredits the system. (See Chapter 14, System Certification and Accreditation.)

8.2 Master and Subordinate IT Security Systems Requirements

8.2.1 Master SSPs shall:

- a. Document the security posture of the master system including the IT security category, system type, the NASA-level security controls, the selection of subordinate system security controls, and contingency requirements which shall be certified and accredited prior to proof-of-concept testing, pilot deployments, or full operational status.
- b. Be registered with the OCIO's IT System Registry.
- c. Identify all subordinate systems under its authority in the SSP.
- d. Track and document information regarding their subordinate systems including their C&A status, POA&M status, date of recertification and reaccreditation, the date of the last review of security controls, and the name of the information system owner.

8.2.2 Subordinate SSPs shall:

- a. Document the inherited master system's IT security category, system type, NASA-level security controls, assessment of overall risk, and contingency requirements. If no master system has been established, the subordinate system shall make the interim security determinations.
- b. Document the security posture of the system.
- c. Document the results of the completed risk assessments for specific (i.e., local or site) risk and environmental conditions, since the results of the risk assessment conducted for the master system are inherited by the subordinate system. If no master system has been established, the subordinate system must complete a full system risk assessment.
- d. Document the certification and accreditation decision which either a full or an interim ATO (IATO), prior to proof-of-concept testing, pilot deployments, or full operational status.
- e. Be registered with the appropriate master system AO or OCIO, if a master system has not been established.
- f. Track the C&A status, the POA&M status, the date recertification and reaccreditation is required, and the date of the last review of security controls.

8.3 Additional Master and Subordinate IT System References

- a. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.
- b. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems.
- c. NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information.

| [TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) |
[Chapter5](#) | [Chapter6](#) | [Chapter7](#) | [Chapter8](#) | [Chapter9](#) | [Chapter10](#) |
[Chapter11](#) | [Chapter12](#) | [Chapter13](#) | [Chapter14](#) | [Chapter15](#) |
[Chapter16](#) | [Chapter17](#) | [Chapter18](#) | [Chapter19](#) | [Chapter20](#) |
[Chapter21](#) | [AppendixA](#) | [AppendixB](#) | [ALL](#) |

| [NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
